

## Office of the Secretary of Defense

## §311.3

### §311.1 Purpose.

This part revises 32 CFR part 311 to update Office of the Secretary of Defense (OSD) and Joint Staff (JS) policy, assigns responsibilities, and prescribes procedures for the effective administration of the Privacy Program in OSD and the JS. This part supplements and implements part 32 CFR part 310, the DoD Privacy Program.

### §311.2 Applicability.

This part:

(a) Applies to OSD, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, and all other activities serviced by Washington Headquarters Services (WHS) that receive privacy program support from OSD/JS Privacy Office, Executive Services Directorate (ESD), WHS (hereafter referred to collectively as the “WHS-Serviced Components”).

(b) Covers systems of records maintained by the WHS-Serviced Components and governs the maintenance, access, change, and release information contained in those systems of records, from which information about an individual is retrieved by a personal identifier.

### §311.3 Definitions.

(a) *Access*. The review of a record or a copy of a record or parts thereof in a system of records by any individual.

(b) *Computer matching program*. A program that matches the personal records in computerized databases of two or more Federal agencies.

(c) *Disclosure*. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government Agency, other than the subject of the record, the subject's designated agent or the subject's legal guardian.

(d) *Individual*. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Members of the United States Armed Forces are “individuals.” Corporations, partnerships, sole proprietorships, professional groups, businesses, whether

incorporated or unincorporated, and other commercial entities are not “individuals” when acting in an entrepreneurial capacity with the Department of Defense but are “individuals” otherwise (e.g., security clearances, entitlement to DoD privileges or benefits, etc.).

(e) *Individual access*. Access to information pertaining to the individual by the individual or his or her designated agent or legal guardian.

(f) *Maintain*. To maintain, collect, use, or disseminate records contained in a system of records.

(g) *Personal information*. Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a social security number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information also is known as *personally identifiable information* (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information which is linked or linkable to a specified individual).

(h) *Record*. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc.), about an individual that is maintained by a WHS-Serviced Component, including, but not limited to, his or her education, financial transactions, medical history, criminal or employment history, and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

(i) *System manager*. A WHS-Serviced Component official who has overall responsibility for a system of records. The system manager may serve at any level in OSD. Systems managers are indicated in the published systems of records notices. If more than one official is indicated as a system manager, initial responsibility resides with the manager at the appropriate level (i.e., for local records, at the local activity).

#### § 311.4

#### 32 CFR Ch. I (7–1–13 Edition)

(j) *System of records.* A group of records under the control of a WHS-Serviced Component from which personal information about an individual is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned, that is unique to the individual.

#### § 311.4 Policy.

It is DoD policy, in accordance with 32 CFR part 310, that:

(a) Personal information contained in any system of records maintained by any DoD organization shall be safeguarded. To the extent authorized by section 552a of title 5, United States Code, commonly known and hereafter referred to as the “Privacy Act” and Appendix I of Office of Management and Budget Circular No. A-130 (available at <http://www.whitehouse.gov/omb/assets/omb/circulars/a130/a130trans4.pdf>), an individual shall be permitted to know what existing records pertain to him or her consistent with 32 CFR part 310.

(b) Each office maintaining records and information about individuals shall ensure that this data is protected from unauthorized collection, use, dissemination and/or disclosure of personal information. These offices shall permit individuals to have access to and have a copy made of all or any portion of records about them, except as provided in 32 CFR 310.17 and 310.18. The individuals will also have an opportunity to request that such records be amended as provided by 32 CFR 310.19. Individuals requesting access to their records shall receive concurrent consideration under section 552 of title 5, United States Code (commonly known and hereafter referred to as the “Freedom of Information Act”).

(c) Necessary records of a personal nature that are individually identifiable will be maintained in a manner that complies with the law and DoD policy. Any information collected by WHS-Serviced Components must be as accurate, relevant, timely, and complete as is reasonable to ensure fairness to the individual. Adequate safeguards must be provided to prevent misuse or unauthorized release of such information, consistent with the Privacy Act.

#### § 311.5 Responsibilities.

(a) The Director, WHS, under the authority, direction, and control of the Director, Administration and Management, shall:

(1) Direct and administer the OSD/JS Privacy Program for the WHS-Serviced Components.

(2) Ensure implementation of and compliance with standard and procedures established in 32 CFR part 310.

(3) Coordinate with the WHS General Counsel on all WHS-Serviced Components denials of appeals for amending records and review actions to confirm denial of access to records.

(4) Provide advice and assistance to the WHS-Serviced Components on matters pertaining to the Privacy Act.

(5) Direct the OSD/JS Privacy Office to implement all aspects of 32 CFR part 310 as directed in § 311.7 of this part.

(b) The Heads of the WHS-Serviced Components shall:

(1) Designate an individual in writing as the point of contact for Privacy Act matters and advise the Chief, OSD/JS Privacy Office, of names of officials so designated.

(2) Designate an official in writing to deny initial requests for access to an individual’s records or changes to records and advise the Chief, OSD/JS Privacy Office of names of officials so designated.

(3) Provide opportunities for appointed personnel to attend periodic Privacy Act training.

(4) Report any new record system, or changes to an existing system, to the Chief, OSD/JS Privacy Office at least 90 days before the intended use of the system.

(5) Formally review each system of records notice on a biennial basis and update as necessary.

(6) In accordance with 32 CFR 310.12, include appropriate Federal Acquisition Regulation clause (48 CFR 24.104) in all contracts that provide for contractor personnel to access WHS-Serviced Component records systems covered by the Privacy Act.

(7) Review all implementing guidance prepared by the WHS-Serviced Components as well as all forms or other methods used to collect information about individuals to ensure compliance with 32 CFR part 310.